Integer estimation methods for GPS ambiguity resolution: an applications oriented review and improvement

AUTHOR(S):

Xu, Peiliang; Shi, Chuang; Liu, Jingnan

Survey Review (2012), 44, 59-71, DOI 10.1179/1752270611Y.0000000004

Integer estimation methods for GPS ambiguity resolution: an applications-oriented review and improvement

Peiliang Xu[1], Chuang Shi[2] and Jingnan Liu[2]
1. Disaster Prevention Research Institute, Kyoto University, Uji, Kyoto 611-0011, Japan
email: pxu@rcep.dpri.kyoto-u.ac.jp
2. GNSS Research Center, Wuhan University, Wuhan 430071, PR China

Abstract: *The integer least squares (ILS) problem, also known as the weighted closest point problem, is highly interdisciplinary but no algorithm can find its global optimal integer solution in polynomial time. We first outline two suboptimal integer solutions, which can be important either in real-time communication systems or to solve high dimensional GPS integer ambiguity unknowns. We clarify that the popular sorted QR suboptimal estimator, usually known to be invented by Wübben et al. [42], was first discussed by Xu et al. [51]. We then focus on the most efficient algorithms to search for the exact integer solution. We show that the combined algorithm proposed by Fincke and Pohst [8] and Schnorr and Euchner [29], which is well known to be the most powerful algorithm for solving the ILS problem, is much faster than LAMBDA in the sense that the ratio of integer candidates to be checked by the combined algorithm to those by LAMBDA can be theoretically expressed by r^m, where $r \leq 1$ and m is the number of integer unknowns. Finally, we further improve the searching efficiency of the most powerful combined algorithm by implementing two sorting strategies, which can either be used for finding the exact integer solution or for constructing a suboptimal integer solution. Test examples clearly demonstrate that the improved methods can perform significantly better than the most powerful combined algorithm to simultaneously find the optimal and second optimal integer solutions, if the ILS problem cannot be well reduced.*

Keywords: global positioning system (GPS), integer linear model, integer least squares, closest point problem, lattice reduction, LLL algorithm.

1 Introduction

Given a number of data y_1, y_2, ..., y_n, each of which being respectively a linear or nonlinear function of real-valued and integer unknown parameters $\boldsymbol{\beta}$ and $\mathbf{z}$, the theory of integer estimation is to optimally estimate both $\boldsymbol{\beta}$ and $\mathbf{z}$ from the data. More specifically, let us start with the following mixed integer linear model:

$$\mathbf{y} = \mathbf{A}\boldsymbol{\beta} + \mathbf{B}\mathbf{z} + \boldsymbol{\epsilon}, \tag{1}$$

where $\mathbf{y}$ is an n-dimensional vector of observations y_1, y_2, ..., y_n, $(\mathbf{A}, \mathbf{B})$ is an $n \times (t+m)$ real-valued matrix of full column rank, $\boldsymbol{\beta}$ is a real-valued vector, i.e., $\boldsymbol{\beta} \in \mathcal{R}^t$ and $\mathbf{z}$ is an integer vector, i.e., $\mathbf{z} \in \mathcal{Z}^m$. Here $\mathcal{R}^t$ is defined as the t-dimensional real-valued space and $\mathcal{Z}^m$ as the m-dimensional integer space. $\boldsymbol{\epsilon}$ is the error vector of the observations $\mathbf{y}$. The mean and variance-covariance matrix of $\boldsymbol{\epsilon}$ are assumed to be zero and $\mathbf{W}^{-1}\sigma^2$, where $\mathbf{W}$ is a given positive definite matrix and σ^2 is an unknown positive scalar. If $\mathbf{A} = \mathbf{0}$, then the mixed integer linear model (1) is simplified as the following integer linear model:

$$\mathbf{y} = \mathbf{B}\mathbf{z} + \boldsymbol{\epsilon}. \tag{2}$$

The problem of estimating the integer unknown vector $\mathbf{z}$ in (1) or (2) arises from multidisciplinary subjects of science and engineering, for example, integer programming, geometry of numbers, multiple-input-multiple-output (MIMO) communication systems and cryptography. If the data $\mathbf{y}$ are free of noise or random errors, the integer linear model (2) defines a lattice with a generator matrix $\mathbf{B}$, namely,

$$\mathcal{L} = \left\{ \sum_{i=1}^{m} \mathbf{b}_i z_i \mid z_i \in \mathbb{Z} \right\}, \tag{3}$$

where $\mathbf{b}_i$ are the column vectors of the matrix $\mathbf{B}$. Obviously, a lattice $\mathcal{L}$ is a discrete point set regularly distributed in the real-valued space $\mathcal{R}^n$, which has been in the center of the theory of geometry of numbers as a branch of pure mathematics and associated with the names of many great mathematicians such as Lagrange, Gauss, Hermite, Minkowski and Voronoi (see, e.g., [13],[28]).

Estimating integer unknowns $\mathbf{z}$ in the integer linear model (2) with random noise has been extensively investigated recently. However, it has been interpreted in different languages in different subjects of study. For example, in communication, one uses the language of coding and decoding in connection with (2). In this case, an MIMO communication system may consist of two components: one to transmit codewords (of integer nature) and the other to decode or recover the transmitted integers from the noise-contaminated received signals (see, e.g., [7],[30]). An optimal decoding system is to minimize the probability of error for the estimated integers. If the random errors $\boldsymbol{\epsilon}$ are assumed to be normally distributed with zero mean, Shannon [30] derived an elegant lower probabilistic bound of error for the maximum likelihood (ML) integer estimator. In cryptography, the language would be on hiding secret information and disclosing/attacking/breaking a cryptosystem (see, e.g., [17],[27]). More examples can be found in the literature of crystallography (see, e.g., [2],[9]) and learning with errors (see, e.g., [27]).

In precise GPS/InSAR positioning applications, $\mathbf{y}$ of (1) has often stood for carrier phase observables, and $\mathbf{z}$ for the integer ambiguity unknown vector. GPS ambiguity resolution is well known to be the key technique to GPS precise positioning. In the geodetic community, Teunissen [34] first addressed the integer estimation problem by developing the decorrelation integer least squares (ILS) method for GPS ambiguity resolution from the point of view of projection theory. Xu et al. [51] alternatively solved the mixed ILS problem by using a two-step approach. Although (1) has been well known in geodetic literature as the standard mathematical model for GPS precise positioning and InSAR unwrapping, the terminology of *GPS observation model* or InSAR unwrapping will hardly be understood by the people who do not work on GPS/InSAR. In particular, since the integer linear model (2) is highly interdisciplinary, Xu *et al.* [51-52] and Xu [44,47-49] have instead called (1) the *mixed integer linear model* and accordingly (2) the *integer linear model*, in order for researchers from different disciplines to communicate with a common terminology.

The estimation of real-valued and integer unknown parameters $\boldsymbol{\beta}$ and $\mathbf{z}$ in (1) is essentially a statistical inference problem. However, almost nothing can be found in any statistical literature and/or statistical journals, except for the maximum likelihood estimation of a single integer parameter that is associated with the binomial and/or Poisson distribution (see, e.g., [6],[21],[32]), as can be readily seen after a quick web search or a quick look at scientific journals on statistics. Although the integer linear model (2) is important in many different areas of science and engineering, likely due to the barrier of different languages used in different subject areas, researchers from different disciplines seem to be hardly aware of theory and methods developed and used beyond his or her own field of study. At least, this is particularly true for researchers in geodesy and navigation, as is very clear from the cited literature in the publications of global navigation satellite systems (GNSS). Thus an interdisciplinary presentation of the theory and methods of integer estimation should be urgently useful and helpful to

build bridges for researchers with backgrounds of different disciplines.

This paper will focus on the estimation theory, methods and algorithms for the integer unknowns in (2), since the LS/ML estimation of the real-valued unknown parameters essentially depends on the integer estimate of $\mathbf{z}$ (see, e.g., [34-35],[51-52]). Emphasis will be on theory, methods and algorithms that can be directly implemented for practical applications in different disciplines. The paper is organized as follows. In Section 2, we will briefly discuss the principle of integer estimation theory and formulate the ILS and/or integer ML estimation problem. Since the ILS problem cannot be solved in polynomial time, we will discuss methods to construct suboptimal integer solutions in Section 3. Reduction and decorrelation techniques will be discussed in Section 4, which have been shown to be very powerful in speeding up the search for the globally optimal ILS/ML solution. For practical applications, Section 5 will first analyze the key components of the most powerful algorithms proposed by Fincke and Pohst [8] and Schnorr and Euchner [29], which essentially include reduction/decorrelation, dynamically shrinking the size of searching window and scanning the integer candidates in the zigzagged manner for each integer unknown. In addition to these key components, we propose implementing the sorted QR and V-BLAST strategies to re-order the integer unknowns $\mathbf{z}$ either on the basis of optimality criteria of maximum conditional weighting or minimum conditional variance. The new components of sorting will be shown to significantly improve the most powerful combined algorithm by Fincke and Pohst [8] and Schnorr and Euchner [29], in particular, when searching for the optimal and second optimal integer solutions.

2 The integer LS/ML problem

As a statistical inference problem, one may apply a certain principle of optimality to estimate the integer unknowns $\mathbf{z}$ in (2) from the noisy measurements $\mathbf{y}$. In general, one would use one of the two popular criteria, namely, (weighted) least squares and maximum likelihood, to estimate $\mathbf{z}$, depending on whether the joint probability density function of $\mathbf{y}$ is available. If the weighted LS method is applied to the integer linear model (2), we have the following ILS problem:

$$\min_{\mathbf{z}\in\mathbb{Z}^m}\quad \mathrm{F}(\mathbf{z})=(\mathbf{y}-\mathbf{B}\mathbf{z})^T\mathbf{W}(\mathbf{y}-\mathbf{B}\mathbf{z}), \tag{4}$$

which can be equivalently rewritten as

$$\min_{\mathbf{z}\in\mathbb{Z}^m}\quad \mathrm{F}(\mathbf{z})=(\mathbf{z}-\mathbf{z}_f)^T\mathbf{W}_f(\mathbf{z}-\mathbf{z}_f), \tag{5}$$

where

$$\mathbf{W}_f=\mathbf{B}^T\mathbf{W}\mathbf{B},$$
$$\mathbf{z}_f=(\mathbf{B}^T\mathbf{W}\mathbf{B})^{-1}\mathbf{B}^T\mathbf{W}\mathbf{y}=\mathbf{W}_f^{-1}\mathbf{B}^T\mathbf{W}\mathbf{y},$$

(see, e.g., [49]). In the GNSS literature, one has more often called $\mathbf{z}_f$ the (real-valued) floating solution (of $\mathbf{z}$) and $\mathbf{W}_f$ its corresponding weight matrix, respectively. In communication, one often assumes that the random errors $\boldsymbol{\epsilon}$ in (2) are normally distributed. Accordingly, (4) can also be derived from the (integer) maximum likelihood principle (see, e.g., [30]).

Although the estimation of integer unknowns is relatively new in geodesy and navigation and was only strictly treated mathematically in the past two decades, the optimization problem (4) or (5) has actually been well known as a convex quadratic integer programming problem beyond the literature of geodesy and navigation. In particular, two special cases of (4) have been extensively investigated in integer programming. As a first special case, if $\mathbf{W}=\mathbf{I}$, then (4) becomes

$$\min_{\mathbf{z}\in\mathbb{Z}^m}\quad \mathrm{F}(\mathbf{z})=(\mathbf{y}-\mathbf{B}\mathbf{z})^T(\mathbf{y}-\mathbf{B}\mathbf{z}), \tag{6}$$

which has been well known as the *closest vector problem* (see, e.g., [22]). As is clear from (3), $\mathbf{Bz}$ defines a lattice. As a result, (6) is also called the *closest point problem* in integer programming (see, e.g., [22]). If we further set $\mathbf{y}$ in (6) to $\mathbf{0}$, the corresponding problem is alternatively called the *shortest vector problem* (see, e.g., [22]). We should note, however, that integer programming is concerned with finding the optimal numerical solution(s) to an objective function with integer variables. It is only an important tool in integer statistical inference associated with (1) and/or (2).

The ILS estimate of $\mathbf{z}$, or equivalently, the solution to (4) or (5) can be represented by the support/indicator function as follows:

$$\hat{\mathbf{z}} = \sum_{\mathbf{z}\in\mathbb{Z}^m} \mathbf{z}\ \mathrm{I}(V(\mathbf{z}), \mathbf{z}_f), \tag{7}$$

(see, e.g., [14],[37],[48-49]), where $\hat{\mathbf{z}}$ is the ILS estimator of the integer vector $\mathbf{z}$, $\mathrm{I}(V(\mathbf{z}), \mathbf{z}_f)$ is the indicator function:

$$\mathrm{I}(V(\mathbf{z}), \mathbf{z}_f) = \begin{cases} 1, & \text{if } \mathbf{z}_f \in V(\mathbf{z}) \\ 0, & \text{otherwise} \end{cases}$$

Here $V(\mathbf{z})$ is the Voronoi cell centered at the point $\mathbf{z}$, whose definition can be found in, e.g., Cassels [3] and Gruber and Lekkerkerker [13]. If $\mathbf{z} = \mathbf{0}$, the corresponding Voronoi cell is denoted by V_0. The construction of V_0 can be found in Sikiric et al. [41] and Xu [49]. For more details on upper and lower probabilistic bounds of correctly estimating the integer unknown vector $\mathbf{z}$ and integer hypothesis testing, the reader is referred to Xu [48].

3 Suboptimal integer solutions

Solving the ILS problem (4) is well known to be NP-hard. In other words, there exists no algorithm to find the global optimal integer solution to (4) in the polynomial time of dimension m (see, e.g., [22]). Thus for real-time applications such as wireless communication and GPS kinematic positioning with many integer ambiguities due to the use of different wavelengths and/or different navigation satellite systems, it may be more realistic to expect some good suboptimal integer solutions than to find the global optimal integer solution to (4). For example, in GPS ambiguity resolution, one can use the noise of code range to determine the size of searching window for each integer ambiguity. The corresponding size of searching window for each z_i may be reasonably assumed to be between 5 and 11 (see, e.g., [16],[18]). In this case, if $m = 60$, then the total number of integer combinations is approximately between $8.67 \times 10^{41} (= 5^{60})$ and $3.04 \times 10^{62} (= 11^{60})$. If the number of $\mathbf{z}$ is increased to 100, the number of combinations can be as large as $1.38 \times 10^{104} (= 11^{100})$. Obviously, in such cases, it is practically not possible to find the exact integer solution.

Suboptimal integer solutions could also be interpreted differently in wireless communication and GNSS. In wireless communication, one would have to decode the received signals which are always changing with time. However, in the case of GNSS kinematic positioning, the integer ambiguities remain unchanged with time, and as a result, one can collect and accumulate more data in order to obtain the global optimal integer solution. In other words, suboptimal integer solutions can be temporary in GNSS and meaningful at a particular point of time, unless the number of integer ambiguities is too big to solve due to the NP-hardness of (4).

Basically, all the methods to construct suboptimal integer solutions may be classified into two types: (i) simple rounding and (ii) sequential rounding. Since the real-valued vector $\mathbf{z}_f$ of (5) is given, the simplest and oldest approach to finding a suboptimal integer solution to (5) is to round each element of $\mathbf{z}_f$ to its nearest integer, namely,

$$\widehat{\mathbf{z}}_{s1} = \lceil \mathbf{z}_f \rfloor, \tag{8}$$

where $\lceil x \rfloor$ stands for rounding x to its nearest integer (see, e.g., [33]). Grafarend [12] suggested applying the integer orthogonalization algorithm to (5) in order to improve the solution quality of the direct rounding suboptimal solution (8). The integer solution (8) is globally optimal, if the positive definite matrix $\mathbf{W}_f$ of (5) is diagonal.

Most of suboptimal integer solutions are sequential. The word "*sequential*" should also be understood differently under different contexts. For example, given all the measurements $\mathbf{y}$, one may *sequentially* estimate one integer sub-optimally, conditional on that the others have been estimated. This is true in the literature of communication, and likely some of the GNSS literature. In kinematic GPS/GNSS positioning or processing GPS networks at a global scale, one may either sequentially fix one integer ambiguity if it is judged to be correct with a very high probability or decide not to fix it. In this latter case, one chooses to accumulate more data and then continue to fix the remaining integer ambiguity unknowns sequentially if such a (conditional) probability is sufficiently high (see, e.g., [1],[5],[10],[20]). More precisely, common practice to derive the suboptimal integer solution is to start with the most accurate component of $\mathbf{z}_f$ and decide whether the integer unknown can be fixed with a sufficiently high probability which is computed as if the integer were a real-valued random variable. For example, assuming that $(i-1)$ integers have been fixed with the conditional probabilities $p_j\,(j = 1, 2, ..., i-1)$, and further assuming that given the new data and $z_j\,(j = 1, 2, ..., i-1)$, the sequential real-valued estimate z_f^k of z_k $(k \in [i, i+1, ..., m])$ is most accurate with a variance σ_k^2, then Blewitt [1] suggested computing the following quantity p_k, which was called the conditional probability and given as follows:

$$p_k = p_{i-1} \exp\{-(z_f^k - \lceil z_f^k \rfloor)^2/(2\sigma_k^2)\} / \sum_{j \in Z} \exp\{-(z_f^k - j)^2/(2\sigma_k^2)\}, \tag{9}$$

where p_1 is set to p_0. If the prior probability p_0 is equal to unity, we presume that the first integer is correctly fixed. If p_k is sufficiently large, one can then fix z_f^k, permutate z_k with z_i and continue to fix the next integer; otherwise, more data are collected and the above procedure is repeated until all the components of $\mathbf{z}$ have been sequentially obtained. Note, however, that in GPS/GNSS applications, the accuracy of the real-valued estimates are often found to be too optimistic. As a result, Blewitt [1] actually replaced σ_k in (9) with $|z_f^k - \lceil z_f^k \rfloor|/2$ approximately. Since this strategy of sequentially estimating suboptimal integer solutions is clear by itself, we shall focus on the approach to constructing suboptimal integer solutions without any new measurements in the remainder of this Section.

All the sequential, suboptimal integer solutions without new data start with the Cholesky decomposition of $\mathbf{W}_f$, namely,

$$\mathbf{W}_f = \mathbf{L}\mathbf{D}\mathbf{L}^T, \tag{10}$$

where $\mathbf{L}$ is a lower triangular matrix with the unit diagonal elements and $\mathbf{D}$ is diagonal with all the diagonal elements being positive. Substituting (10) into (5) yields

$$\min_{\mathbf{z} \in \mathbb{Z}^m} \quad \mathrm{F}(\mathbf{z}) = \sum_{i=1}^{m} d_{ii} \left\{ z_i + \sum_{j=i+1}^{m} l_{ji}(z_j - z_j^f) - z_i^f \right\}^2, \tag{11}$$

where $l_{ij}\,(j < i)$ are the non-zero, off-diagonal elements of $\mathbf{L}$ and d_{ii} the positive diagonal elements of $\mathbf{D}$. z_i^f is the ith element of the real-valued vector $\mathbf{z}_f$. In order to avoid solving the NP-hard integer optimization problem (11), one may seek only a suboptimal solution with least possible work. One obvious solution is to simply minimize all the terms $|z_i + \sum_{j=i+1}^{m} l_{ji}(z_j - z_j^f) - z_i^f|$ with respect to z_i, given the integers $z_j\,(j > i)$. As a result, the suboptimal integer solution can be readily represented by

$$\hat{z}_{s2}^i = \lceil z_i^f - \sum_{j=i+1}^{m} l_{ji}(\hat{z}_{s2}^j - z_j^f) \rfloor \tag{12}$$

with i running from m to 1, where $\hat{z}_{s2}^{i}$ is the ith component of the suboptimal sequential integer estimator of $\mathbf{z}$.

The representation of the suboptimal integer solution (12) was derived by Xu et al. [51], which can serve as a starting point to construct any sequential suboptimal integer solution. However, the quality of a suboptimal solution of type (12) can be quite different, depending on the ordering of the estimation of each component of $\mathbf{z}$. In other words, constructing a good suboptimal integer solution is now equivalent to designing an optimal ordering to Cholesky-decompose $\mathbf{W}_f$ in (10) and accordingly obtain readily the solution of type (12). In the original contribution by Xu et al. [51], they proposed incorporating the reduction process into the decomposition of $\mathbf{W}_f$, which is carried out by always choosing and pivoting the smallest diagonal element among the remaining diagonal elements to be decomposed.

In the literature of communication, there exist two most popular ordering techniques to construct suboptimal integer solutions, which are the QR sorting (see, e.g., [38],[42-43],[51-52]) and the *V*ertical *B*ell *L*abs *L*ayered *S*pace-*T*ime (V-BLAST) ordering (see, e.g., [11],[39]). These two ordering techniques are based on the QR decomposition of the design matrix $\mathbf{B}$ and the variance-covariance matrix of the real-valued solution $\mathbf{z}_f$, respectively. Other improvement can be found, for example, in Waters and Barry [38].

For the integer linear model (2) without any new data, and by assuming that the weight matrix $\mathbf{W}$ of $\mathbf{y}$ is an identity matrix, namely, $\mathbf{W} = \mathbf{I}$, Wübben et al. [42] proposed applying the Gram-Schmidt orthogonalization procedure to $\mathbf{B}$ in such a way that the vectors to be orthogonalized are all projected onto the orthogonal complement of the completed orthogonalized vectors and then the shortest vector is picked up to resume the next orthogonalization process. The procedure described is called the sorted QR decomposition. Accordingly, the ordering obtained is called the QR-sorting. As a result, (2) can be rewritten as follows:

$$\mathbf{y} = \mathbf{QRPz} + \boldsymbol{\epsilon}.$$

Or equivalently,

$$\mathbf{y}_q = \mathbf{R}\mathbf{z}_q + \boldsymbol{\epsilon}_q, \tag{13}$$

where

$$\mathbf{z}_q = \mathbf{P}\mathbf{z},$$
$$\mathbf{y}_q = \mathbf{Q}^T\mathbf{y},$$
$$\boldsymbol{\epsilon}_q = \mathbf{Q}^T\boldsymbol{\epsilon},$$

and $\mathbf{P}$ is a permutation matrix.

Because $\mathbf{W} = \mathbf{I}$, the corresponding ILS problem of (13) becomes

$$\min_{\mathbf{z}_q \in \mathbb{Z}^m} \quad \mathrm{F}(\mathbf{z}_q) = (\mathbf{z}_q - \mathbf{z}_f^q)^T\mathbf{R}^T\mathbf{R}(\mathbf{z}_q - \mathbf{z}_f^q), \tag{14}$$

where $\mathbf{z}_f^q = (\mathbf{R}^T\mathbf{R})^{-1}\mathbf{R}^T\mathbf{y}_q$. Since $\mathbf{R}$ is upper-triangular, (14) is essentially the same as (11) and one can immediately obtains the same suboptimal integer estimator as represented by (12).

However, if $\mathbf{W}$ is not an identity matrix, then one cannot directly apply the sorted QR decomposition to $\mathbf{B}$. The reason is simple: if $\mathbf{W} \neq \mathbf{I}$, $(\mathbf{R}^T\mathbf{R})$ in (14) has to be replaced by $(\mathbf{R}^T\mathbf{Q}^T\mathbf{WQR})$. The sorted QR decomposition of $\mathbf{B}$ does not make sense because of a non-identity matrix $\mathbf{W}$. In this case, one has to directly work on the normal matrix $\mathbf{W}_f$ instead of $\mathbf{B}$, as done by Xu et al. [51]. Although the sorted QR suboptimal integer estimator is now very popular in the literature of communications, as evidenced by a long list of its citing publications, it is trivial to prove that the sorted QR technique

proposed by Wübben et al. [42-43] is essentially equivalent to the sorting strategy used by Xu et al. [51] for the positive definite matrix $\mathbf{W}_f$. Thus the suboptimal solution by Wübben et al. [42-43] is a special case of Xu et al. [51-52]. Actually, Xu et al. [51-52] went further than Wübben et al. [42] on two accounts: (i) Xu et al. [51] worked on $(\mathbf{B}^T\mathbf{W}\mathbf{B})$. Thus unlike Wübben et al. [42], the weight matrix $\mathbf{W}$ is not an issue of concern here; and (ii) Xu et al. [51] implemented the reduction/decorrelation directly into the procedure of constructing the suboptimal sorted QR integer solution, which should make the sorted QR suboptimal integer solution proposed by Xu et al. [51] more efficient or powerful than the one by Wübben et al. [42]. An algorithm for this most general case is given in Algorithm 1 for convenience of implementation (see, e.g., [50]).

Algorithm 1: Cholesky decomposition with the sorted QR ordering

---

Set L to an identity matrix;
for $i = 1$ **to** m - 1
  get the smallest w_{kk}^f among w_{jj}^f $(i \le j \le m)$;
  if $i \neq k$
    Swap $L(i, 1:i-1)$ with $L(k, 1:i-1)$;
    Swap the elements of submatrix $\mathbf{W}_f(i:m, i:m)$,
      both at the ith and kth row and column;
  end
  Compute $L(i+1:m, i) = \mathbf{W}_f(i+1:m, i)/w_{kk}^f$;
  $D(i,i) = w_{kk}^f$;
  Update $\mathbf{W}_f(i+1:m, i+1:m)$ with $L(i+1:m, i)$ and w_{kk}^f;
end
$D(m,m) = \mathbf{W}_f(m,m)$.

The other popular ordering technique, namely, the V-BLAST sorting, is to focus on the inverse of $\mathbf{W}_f$ instead of $\mathbf{W}_f$ itself. It was first proposed by a group of researchers with Bell Laboratories (see, e.g., [11]) and has since been widely used to construct a suboptimal integer solution of $\mathbf{z}$ (see, e.g., [39],[43]). Following Golden et al. [11], if $\mathbf{W} = \mathbf{I}$, then the V-BLAST ordering is obtained by finding an index k_i such that

$$\min_{j \notin \{k_1, k_2, ..., k_{i-1}\}} \quad \mathrm{F}(j) = \|\mathbf{h}_j\|, \tag{15}$$

where $\mathbf{h}_j$ is the jth row vector of $(\mathbf{B}_{k_i}^T\mathbf{B}_{k_i})^+\mathbf{B}_{k_i}^T$, $\mathbf{B}_{k_i}$ is the matrix of $\mathbf{B}$ by setting all the columns with the indices $\{k_1, k_2, ..., k_{i-1}\}$ to zero, the superscript + stands for the Moore-Penrose pseudoinverse of a matrix.

Actually, if $\mathbf{W} = \mathbf{I}$, the minimization (15) is statistically equivalent to picking up the index such that the real-valued solution of the corresponding integer parameter z_{k_i} is the most precise on the condition that the parameters $\{z_{k_1}, z_{k_2}, ..., z_{k_{i-1}}\}$ have been correctly determined. For conciseness of notations, we denote the submatrix of $\mathbf{B}$ without $\{z_{k_1}, z_{k_2}, ..., z_{k_{i-1}}\}$ by $\mathbf{B}_p$ and accordingly the subvectors of the integer parameters by $\mathbf{z}_p$. Thus, the real-valued solution of $\mathbf{z}_p$, denoted by $\mathbf{z}_f^p$, is written as follows:

$$\mathbf{z}_f^p = (\mathbf{B}_p^T\mathbf{B}_p)^{-1}\mathbf{B}_p^T\mathbf{y}. \tag{16}$$

The variance-covariance matrix of $\mathbf{z}_f^p$ is

$$D(\mathbf{z}_f^p) = (\mathbf{B}_p^T\mathbf{B}_p)^{-1}\mathbf{B}_p^T\mathbf{B}_p(\mathbf{B}_p^T\mathbf{B}_p)^{-1} = (\mathbf{h}_j\mathbf{h}_l^T) = (\mathbf{B}_p^T\mathbf{B}_p)^{-1}. \tag{17}$$

In other words, the solution to the minimization problem (15), as represented by one of the diagonal elements of $(\mathbf{h}_j^T\mathbf{h}_l)$, corresponds exactly to the index of $\mathbf{z}_f^p$ such that its diagonal element of $(\mathbf{B}_p^T\mathbf{B}_p)^{-1}$ is minimum. From this point of view, although the V-BLAST ordering proposed by Golden et al. [11]

assumed an identity matrix, we can naturally extend it to a most general weight matrix $\mathbf{W}$. As a result, the ordering algorithm given by Golden et al. [11] can be substantially simplified and coded in Algorithm 2 to construct the suboptimal integer solution.

Algorithm 2: Finding the V-BLAST ordering

Given $\mathbf{B}$ and $\mathbf{W}$ and initialize $S = \{0\}$;
for $i = 1$ **to** m - 1
  Find the index k_i of z_{k_i} with the smallest diagonal element of $D(\mathbf{z}_f^p)$;
  Assign k_i to the set $S = \{k_1, k_2, ..., k_{i-1}, k_i\}$
  Form $\mathbf{B}_p$ by deleting the columns of $\mathbf{B}$ in S;
  Compute $D(\mathbf{z}_f^p)$;
end
Assign the remaining index to the set $S = \{k_1, k_2, ..., k_m\}$

If we compare Algorithm 2 with that by Golden et al. [11], we can readily find that Algorithm 2 is advantageous: (i) it is computationally less complex, since the $D(\mathbf{z}_f^p)$-equivalent Moore-Penrose pseudoinverse in (15) is all what we need; (ii) the dimension of the inverse $D(\mathbf{z}_f^p)$ is smaller than the Moore-Penrose pseudoinverse in (15); and (iii) the weight matrix $\mathbf{W}$ is not necessarily an identity matrix. We should note that this strategy is equivalent to the sequential adjustment/fixing technique, as well mentioned and implemented in the GNSS literature (see, e.g., [1],[5],[20]), if all the integer unknowns can be fixed with a high probability. However, if a GPS integer ambiguity unknown cannot be fixed and more data are to be collected before a sequential adjustment can be continued, then the suboptimal solution proposed by Golden et al. [11] is different from the sequential adjustment/fixing technique used in GNSS positioning and navigation. The results reported by Wübben et al. [42] have shown that the V-BLAST ordering performs better than the sorted QR ordering in terms of error performance. The sorted QR ordering requires much less computation, nevertheless.

4 Reduction and decorrelation

Reduction has been an important tool in number theory. The goal of reduction can now be described to transform the basis of the lattice $\mathcal{L}$ in (3) defined by the column vectors of $\mathbf{B}$ such that the reduced basis is as short as possible and as orthogonal as possible. According to Scharlau and Opolka [28], Lagrange was the first mathematician to investigate the problem of integer binary quadratic forms in 1773, which was also solved in an algorithmically operational way by Gauss in his 1801 book "*Disquisitiones Arithmeticae*" (see, e.g., [28],[40]). An algorithm of reduction of quadratic forms in an arbitrary dimension was first constructed by Hermite (see, e.g., [25],[28]). Further development of reduction of quadratic forms and number theory finally led Minkowski to create the subject of geometry of numbers (see, e.g., [28]).

Although reduction of quadratic forms and lattice basis vectors was substantially investigated in the eighteenth and nineteenth centuries by several talent mathematicians such as Gauss, Hermite, Minkowski and Voronoi (see, e.g., [13],[28]), a landmark reduction algorithm was invented by A. *L*enstra, H. *L*enstra and L. *L*ovász (1982). It has since been popularized as the LLL algorithm coined after the three *L*s in the authors' family names and widely applied in many areas of science and engineering (see, e.g., [26]). Further development has been along the line of either improving the efficiency and stability of computation (see, e.g., [24-25]) or aiming at refining the output quality of the reduced basis through the implementation of deep insertions (see, e.g., [29]). Because the LLL variant with deep insertions is of super-exponential complexity, it will not be included in this paper. The interested reader should refer to Schnorr and Euchner [29]. In this section, we will focus on reduction

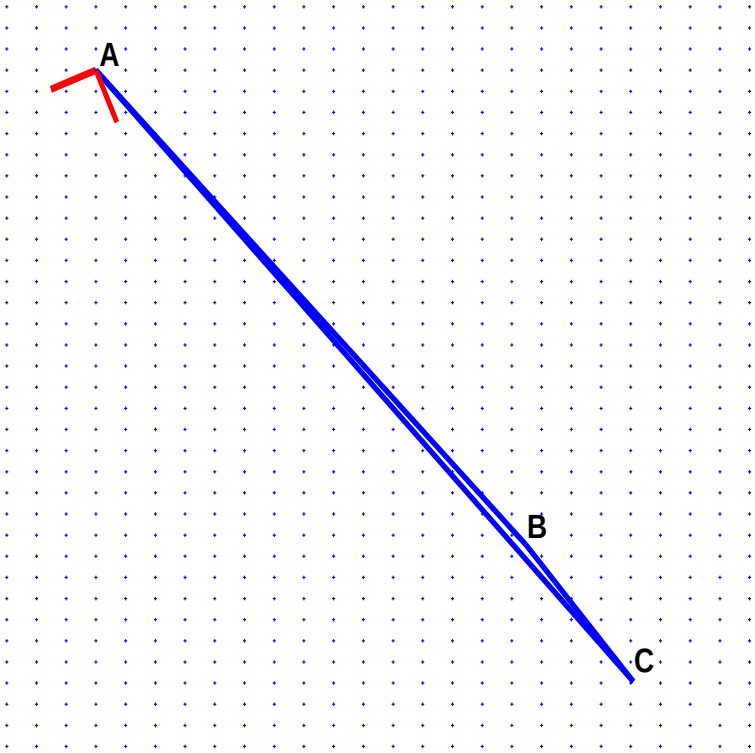

Figure 1: Illustration of a very thin triangle ABC. In terms of lattice, its basis can be formulated by the two directed lines AB and AC, which are far from orthogonal. After applying the LLL algorithm to AB and AC, we obtain the new basis, whose vectors are almost orthogonal and very short, as shown in red lines.

algorithms of practical significance with a polynomial time of complexity.

4.1 The LLL algorithm

The LLL algorithm of lattice basis reduction was constructed by Lenstra et al. [19]. According to the historical account of the LLL algorithm by Smeets [31], its invention started with the question posed to H. Lenstra for handling skewed lattices, which is essential to check whether there exist points with integer coordinates inside a triangle defined by three arbitrary points A, B and C on the plane in polynomial time. Although the answer to this question seems to be trivial, it can actually be very difficult to answer, if the triangle ABC looks almost like a very thin line, as illustrated in Fig.1 of this paper or Fig.1.2 of Smeets [31]. The answer to this question was roughly equivalent to turning the two neighboring directed lines (vectors) of the triangle as orthogonal as possible through a unimodular transformation.

To start with, we assume that the basis vectors $\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_m$, namely, the column vectors of $\mathbf{B}$, are linearly independent for the lattice $\mathcal{L}$ defined by (3). It is obvious from the definition of the lattice (3) that the bases of $\mathcal{L}$ are not unique. In fact, any basis of the type $\mathbf{BG}$ is also a basis of $\mathcal{L}$, where $\mathbf{G}$ is a unimodular matrix. However, some bases are better than others for solving problems of theoretical and practical importance. For example, the basis shown in the red lines in Fig.1, which is obtained after applying the LLL algorithm, would be superior to the original basis with the vectors AB and AC in answering the question posed to H. Lenstra in the above.

Reduction of the lattice basis $\mathbf{B}$ is to find an optimal unimodular transformation matrix $\mathbf{G}$ such that the new basis $\mathbf{B}_r = \mathbf{BG}$ is optimal in a certain sense of optimality. As a result, $\mathbf{G}$ can be solved as the optimal solution to the optimization model formulated under the defined optimality,

and the sense of reduction should be understood accordingly. For example, reduction in the sense of Hermite, Korkine-Zorotareff and Minkowski requires that the first reduced vector be the shortest, subject to some extra inequality constraints (see, e.g., [3],[13],[15]). The formulated objective function is essentially equivalent to the shortest lattice vector problem, subject to the same inequality constraints. If the optimality is defined in the sense that all the (column) vectors of the new basis $\mathbf{B}_r = \mathbf{BG}$ are the mutually most orthogonal and the shortest, reduction is mathematically equivalent to finding an optimal unimodular matrix $\mathbf{G}$ such that the vectors of the reduced basis $\mathbf{B}_r$ are ideally orthogonal and their lengths are all minimized. Obviously, this is an integer multi-objective optimization model and, in principle, can be solved by using techniques of integer multi-objective optimization (see, e.g., [46]). Unfortunately, for a general reduction problem, all the objectives formulated this way can be in conflict and one should not expect the existence of the global optimal integer solution of $\mathbf{G}$ to simultaneously minimize all the objectives formulated. On the other hand, very often, reduction is only a means to help solve problems of theoretical and/or practical importance, e.g., to find the global optimal ILS solution to (4). From this point of view, it may not make much sense to spend a lot of time in order to solve an optimal unimodular matrix $\mathbf{G}$ to the integer multi-objective optimization model. Instead, it is highly desirable to develop fast reduction algorithms to construct an effective unimodular matrix $\mathbf{G}$ without formulating and solving integer optimization problems, with the LLL algorithm as the most outstanding and successful example.

Actually, all reduction methods for lattice basis vectors are based on the Gram-Schmidt orthogonalization process, but they can be different in the way to achieve further reduction of the lengths of the reduced vectors. In the case of the LLL algorithm, it naturally attempts to realize the first reduction goal of mutual orthogonality of the reduced vectors through the following Gram-Schmidt orthogonalization process,

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \mathbf{b}_j^*, \tag{18a}$$

$$\mu_{ij} = \frac{\mathbf{b}_i^T \mathbf{b}_j^*}{\|\mathbf{b}_j^*\|^2}, \tag{18b}$$

where $\|\cdot\|$ stands for the Euclidean L_2-norm of a vector. In general, μ_{ij} can take on a real value of any size. In order to materialize the second reduction goal of making the reduced vectors as short as possible, the LLL algorithm demands the following condition of size reduction

$$|\mu_{ij}| \le 1/2, \tag{18c}$$

for all $1 \le j < i \le m$. In case that the size reduction (18c) is not satisfied for any $j(< i)$, i.e., $|\mu_{ij}| > 1/2$, then $\mathbf{b}_i$ is replaced with $(\mathbf{b}_i - \lceil \mu_{ij} \rfloor \mathbf{b}_j)$, where $\lceil \mu_{ij} \rfloor$ stands for the integer nearest to μ_{ij}.

In order to further reduce the sizes/lengths of the reduced basis vectors, the LLL algorithm imposes the Lovász condition:

$$\delta \|\mathbf{b}_{i-1}^*\|^2 \le \|\mathbf{b}_i^* + \mu_{i(i-1)} \mathbf{b}_{i-1}^*\|^2 \tag{19}$$

for all $1 < i \le m$, where $\delta \in (1/4, 1)$. While the process (18) of orthogonalitization and size reduction proceeds, the Lovász condition (19) will decide whether it should be temporarily suspended for interference. More precisely speaking, if the Lovász condition (19) is violated, Lenstra et al. [19] suggested swapping $\mathbf{b}_i$ with $\mathbf{b}_{i-1}$ before the orthogonalization-reduction process (18) is re-activated. Note, however, that the process index i should be set back to $(i-1)$. In the original LLL algorithm, δ was set to 3/4. For convenience of reference and/or implementation, we list the pseudo-codes of the LLL algorithm in Algorithm 3.

Algorithm 3: Pseudo-codes of the LLL algorithm

S1 **Input:** the basis of lattice $\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_m$
S2 **Initialize:** $k = 2$ and $\mathbf{b}_1^* = \mathbf{b}_1$
S3 **while** $k \leq m$
S4 **for** $j = (k-1)$ **to** 1 **step** -1
S5 compute μ_{kj}
S6 **if** $|\mu_{kj}| > 0.5$
S7 set μ_{kj} to its nearest integer $\lceil \mu_{kj} \rfloor$
S8 replace $\mathbf{b}_k = \mathbf{b}_k - \lceil \mu_{kj} \rfloor \mathbf{b}_j$ and $\mu_{kj} = \mu_{kj} - \lceil \mu_{kj} \rfloor$
S9 **end**
S10 **end**
S11 compute $\mathbf{b}_k^*$
S12 **if** Lovasz's test (19) is true, continue to next k
S13 **else** swap $\mathbf{b}_k$ with $\mathbf{b}_{k-1}$ and set $k = \min(k-1, 2)$
S14 **end**
S15 **end**

4.2 Reduction of positive definite quadratic forms

A positive definite quadratic form is equivalent to a lattice basis up to a rotation and can be interpreted geometrically in terms of lattice bases (see, e.g., [13]). Actually, the reduction of binary positive definite quadratic form was first addressed by Lagrange in 1773 and solved by Gauss in 1801 (see, e.g., [28]). A (2×2) positive definite matrix

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

is said to be reduced in the sense of Lagrange and Gauss, if the following inequalities hold true,

$$a_{11} \leq a_{22}, \tag{20a}$$

$$|a_{12}| \leq a_{11}/2, \tag{20b}$$

(see, e.g., [23],[40]). Usefulness/importance of the two-dimensional Lagrange-Gauss' algorithm of reduction for GPS ambiguity resolution was demonstrated by Teunissen [35] through the Gaussian elimination. Xu et al. [51] proved that the reduction by repeating the integer Gaussian elimination process converges for any $(m \times m)$ positive definite matrix as a direct consequence of Hadamard's inequality.

Since reduction of positive definite quadratic forms only plays an accessory role in helping solve the ILS problem (5), it is certainly not the final goal to be achieved. As in the case of lattice basis reduction, we should avoid formulating reduction of positive definite quadratic forms as an integer (multi-)objective optimization model. Though we use the word "*accessory*" to describe reduction, we do not mean that it is not important. Actually, a good reduction can speed up finding the global optimal integer solution to (5), as can be clearly seen from the experiments by Fincke and Pohst [8]. Thus, we will focus on efficient heuristic approaches of reduction of positive definite quadratic forms, as in the case of the LLL algorithm. If the reader is interested in Minkowski's and/or Korkine-Zorotareff's reductions, he or she may refer to Gruber and Lekkerkerker [13] and Helfrich [15].

In principle, all heuristic algorithms of lattice basis reduction can be directly applied to reduce a positive definite quadratic form. For example, in the case of the LLL algorithm, we can first decompose the positive definite matrix $\mathbf{W}_f$ of (5) into $\mathbf{V}^T\mathbf{V}$, apply the LLL algorithm to $\mathbf{V}$ and obtain the reduced basis $\mathbf{V} = \mathbf{V}_r\mathbf{G}$, where $\mathbf{V}_r$ is the reduced basis of $\mathbf{V}$ and $\mathbf{G}$ the corresponding unimodular matrix. As a result, the ILS problem (5) can be rewritten as

$$\min_{\mathbf{z}_g \in \mathbb{Z}^m}: \quad \mathrm{F}(\mathbf{z}_g) = (\mathbf{z}_g - \mathbf{z}_f^g)^T \mathbf{W}_r (\mathbf{z}_g - \mathbf{z}_f^g), \tag{21}$$

where $\mathbf{z}_g = \mathbf{G}\mathbf{z}$, $\mathbf{z}_f^g = \mathbf{G}\mathbf{z}_f$ and $\mathbf{W}_r = \mathbf{V}_r^T\mathbf{V}_r$. In the remainder of this section, we will discuss two reduction algorithms, which can be applied to directly reduce the positive definite matrix $\mathbf{W}_f$. Algorithms of this type are also known in geodesy as *decorrelation*.

4.2.1 Reduction of positive definite matrices by Gaussian elimination

Although the original works by Lagrange and Gauss are now well known in many areas of science and engineering, they seem to remain unknown or unheard to many of geodesists. Xu et al. [51-52] extended the idea of Lagrange-Gauss's reduction algorithm to an arbitrary dimension m, which can be summarized by the following lemma and theorem.

Lemma 1 (Hadamard's inequality): *For any positive definite matrix* $\mathbf{P}$, *the following inequality*

$$det(\mathbf{P}) \leq \prod p_{ii} \tag{22}$$

holds true. Here p_{ii} *are the diagonal elements of* $\mathbf{P}$.

Theorem 1: *For any positive definite matrix* $\mathbf{P}$, *there exists a unimodular matrix* $\mathbf{G}$ *such that*

$$\mathbf{P} = \mathbf{G}\mathbf{H}\mathbf{G}^T, \tag{23}$$

where $\mathbf{H}$ *is positive definite, too, and satisfies*

$$|h_{ij}| \leq \frac{1}{2}\, min(h_{ii},\ h_{jj}) \quad \forall\ i, j\ \ \&\ \ i \neq j. \tag{24}$$

Lemma 1 is well known, since it is actually the famous Hadamard's inequality. Based on the Hadamard's inequality, it is rather easy to prove Theorem 1. If the reader is interested in the proof, he or she should refer to Xu et al. [51-52] or Xu [44].

In fact, if we follow the Lagrange-Gauss's approach to reducing the positive definite matrix $\mathbf{W}_f$ in association with the ILS problem (5), we can then construct a heuristic algorithm to find the unimodular matrix $\mathbf{G}$ by multiplying a series of unimodular matrix of the following type:

$$\mathbf{G}_{ij} = \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & \vdots & & \ddots & & \\ & & -\lceil w_{ij}^f / w_{ii}^f \rfloor & \cdots & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{bmatrix},$$

if $w_{ii}^f \leq w_{jj}^f$, or

$$\mathbf{G}_{ij} = \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & \cdots & -\lceil w_{ij}^f / w_{jj}^f \rfloor & & \\ & & & \ddots & \vdots & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{bmatrix},$$

if $w_{jj}^f < w_{ii}^f$, where w_{ij}^f are the elements of $\mathbf{W}_f$. When the above procedure converges, we can readily obtain the transformed ILS problem (21) after reduction or decorrelation. Recently, Chang et al. [4] proposed a modified decorrelation/reduction algorithm in order to speed up the least squares ambiguity decorrelation adjustment method proposed by Teunissen [36].

4.2.2 Decorrelation of positive definite matrices by integer Cholesky decomposition

As is well known, the integer solution of (5) can be trivially obtained, if the matrix $\mathbf{L}$ of (10) is unimodular. Unfortunately, given a general ILS problem (5), the off-diagonal elements $l_{ij}\,(j<i)$ of $\mathbf{L}$ are not integers and $\mathbf{L}$ is not unimodular. The question now is how to construct a unimodular matrix $\mathbf{G}$ such that $\mathbf{G}\mathbf{W}_f\mathbf{G}^T$ becomes as diagonal as possible. The first approach to constructing a unimodular matrix $\mathbf{G}$ from $\mathbf{L}$ was implicitly implemented to size-reduce the real-valued matrix of Gram-Schmidt coefficients in the LLL algorithm by Lenstra et al. [19], which can be stated in the following proposition. For more details on Proposition 1 and its algorithmic realization, the reader can refer to Xu [50].

Proposition 1: *For any real-valued lower-triangular matrix* $\mathbf{L}$ *of type (10), there exists a unimodular matrix* $\mathbf{G}$ *such that*

$$\mathbf{L}=\mathbf{G}\mathbf{L}_{\mu}, \tag{25a}$$

where

$$\mathbf{L}_{\mu}=\begin{bmatrix} 1 & & & & \\ \mu_{21} & 1 & & & \\ \mu_{31} & \mu_{32} & 1 & & \\ \vdots & \vdots & \vdots & \ddots & \\ \mu_{m1} & \mu_{m2} & \mu_{m3} & \cdots & 1 \end{bmatrix}, \tag{25b}$$

and all the elements μ_{ij} *satisfy*

$$|\mu_{ij}|\le 0.5,\quad (i>j).$$

Intuitively, one may also round all the off-diagonal elements of $\mathbf{L}$ to their nearest integers and accordingly, construct the unimodular matrix $\mathbf{L}_{in}$. As a result, we can transform $\mathbf{W}_f$ into

$$\mathbf{H}_1=\mathbf{L}_{in}^{-1}\mathbf{L}\mathbf{D}\mathbf{L}^T(\mathbf{L}_{in}^{-1})^T. \tag{26}$$

It is obvious from (26) that $\mathbf{L}_{in}^{-1}\mathbf{L}$ should be ideally an identity matrix or at least, as close to an identity matrix as possible, if we want to have an almost diagonal $\mathbf{H}_1$. Xu [45] argued that directly rounding the elements of $\mathbf{L}$ and then inverting the unimodular matrix $\mathbf{L}_{in}$ was not a good practice to make $\mathbf{L}_{in}^{-1}\mathbf{L}$ become close to an identity matrix. Alternatively, he proposed inverting $\mathbf{L}$ first and then rounding the elements of $\mathbf{L}^{-1}$ to their nearest integers, which is denoted by $\mathbf{L}_{iin}$. Thus $\mathbf{W}_f$ can be transformed into

$$\mathbf{H}=\mathbf{L}_{iin}\mathbf{L}\mathbf{D}\mathbf{L}^T[\mathbf{L}_{iin}]^T. \tag{27}$$

By replacing $\mathbf{W}_f$ with $\mathbf{H}$ and repeating the above procedure, one can then construct the unimodular matrix $\mathbf{G}$, which was called inverse integer Cholesky decorrelation by Xu [45]. When $\mathbf{L}_{iin}$ is an identity matrix, the iteration process is terminated and the unimodular matrix that minimizes the condition number is chosen. Recently, a parallel reduction algorithm for positive definite quadratic forms was proposed by Xu [50], which was demonstrated to perform significantly better than the LLL algorithm.

5 A practical reduction-aided integer LS/ML method

Although the ILS problem (5) is NP-hard, one can still expect to find the exact integer solution, if the number of integer unknowns is not too large, depending on the sizes of searching windows of $\mathbf{z}$ and the computational capacity of a computer. There exist two popular methods to search for the exact global optimal integer solution to (5). One method is to set a fixed size of searching window for each z_i and then search for the exact integer solution within the pre-determined rectangle of $\mathbf{z}$. The sizes of searching windows can either be determined by the noise level of $\mathbf{z}_f$, as often used in the early literature

on GPS ambiguity resolution (see, e.g., [16],[18]), or alternatively by the length of the shortest reduced vector and those of the shortest vectors of the sub-lattices $\mathcal{L}_i$ $(i = 1, 2, \ldots m)$ from $\mathcal{L}$. The other method was originally formulated in Fincke and Pohst [8] and partially used by Teunissen [35-36]. The basic idea of Fincke and Pohst [8] is to first reduce/decorrelate the ILS problem (5) and then use a shrinking strategy to dynamically reduce the size of searching window for each integer unknown. This algorithm was further improved by Schnorr and Euchner [29], who suggested scanning the candidates of each integer in a zigzagged manner from the center, instead of scanning from one end to the other end implemented by Fincke and Pohst [8] (see also [36]). The combined effort by Fincke and Pohst [8] and Schnorr and Euchner [29] has since been turned out to be the most successful/powerful hybrid algorithm to find the exact global integer solution to the ILS problem (5).

In this section, we will first focus on the combined approach of Fincke and Pohst [8] and Schnorr and Euchner [29] to solve (5). This combined searching strategy was used to solve GPS ambiguity resolution by Chang et al. [4]. However, the methods proposed by Fincke and Pohst [8] and Schnorr and Euchner [29] are based on different methods of reduction or decorrelation. In order to further improve the most powerful combined algorithm by Fincke and Pohst [8] and Schnorr and Euchner [29], we will propose the inclusion of two sorting strategies, namely, the sorted QR and V-BLAST ordering scheme, into the combined algorithm, either to construct a suboptimal integer solution or to find the exact integer solution.

The method to solve the ILS problem (5) by Fincke and Pohst [8] is to reformulate (5) with the ellipsoidal constraint as follows:

$$\min_{\mathbf{z} \in \mathbb{Z}^m}: \quad \mathrm{F}(\mathbf{z}) = (\mathbf{z} - \mathbf{z}_f)^T \mathbf{W}_f (\mathbf{z} - \mathbf{z}_f), \tag{28a}$$

subject to

$$(\mathbf{z} - \mathbf{z}_f)^T \mathbf{W}_f (\mathbf{z} - \mathbf{z}_f) \leq C, \tag{28b}$$

where C is a properly given positive constant such that the inequality constraint (28b) is feasible with respect to the integers $\mathbf{z}$. One such value of C can simply be obtained by using the suboptimal solution techniques of Section 3. In order to speed up the searching for the global integer solution to (5), Fincke and Pohst [8] suggested applying reduction methods to reduce $\mathbf{W}_f$ or equivalently a lattice basis corresponding to $\mathbf{W}_f$ before solving (28). They found that the LLL algorithm is the most efficient when compared with a few other reduction algorithms. The same idea of decorrelation was utilized by Teunissen [35-36] in GPS ambiguity resolution. Other decorrelation/reduction techniques can be found in Xu [45],[50]. Thus in the remainder of this section, without loss of generality, we can assume that $\mathbf{W}_f$ of (28) has been reduced and we will search for the global optimal integer solution to this reduced version of (28).

The basic idea of the searching method by Fincke and Pohst [8] is essentially equivalent to dynamically shrinking the lower and upper bounds of searching window for each z_i, based on the Cholesky decomposition of the reduced $\mathbf{W}_f$ and given a progressively improved constraint constant C_{im}. Without loss of generality, we can assume that the reduced $\mathbf{W}_f$ has been decomposed into (10). Thus, given an improved constant C_{im} with an intermediate integer solution $\mathbf{z}_{im}$, the ellipsoidal constraint (28b) can be rewritten as follows:

$$\sum_{i=1}^{m} d_{ii} \left\{ z_i + \sum_{j=i+1}^{m} l_{ji}(z_j - z_j^f) - z_i^f \right\}^2 \leq C_{im}, \tag{29}$$

where C_{im} is equal to C at the beginning of searching. Accordingly, let us denote the searching window

with the value of C by $[\underline{z}_i^0, \overline{z}_i^0]$ for each component of $\mathbf{z}$. Obviously, from (29), we must have

$$d_{mm}(z_m - z_m^f)^2 \leq C_{im}, \tag{30}$$

from which we can readily determine the lower and upper bounds of searching window for z_m as follows:

$$\underline{z}_m = \lfloor -\sqrt{C_{im}/d_{mm}} + z_m^f \rfloor, \tag{31a}$$

$$\overline{z}_m = \lceil \sqrt{C_{im}/d_{mm}} + z_m^f \rceil, \tag{31b}$$

where $\underline{z}_m$ and $\overline{z}_m$ are the lower and upper integer bounds of z_m, respectively. $\lfloor x \rfloor$ stands for the integer not larger than x and $\lceil x \rceil$ for the integer not smaller than x, respectively.

If the searching of z_m at the previous iteration has gone beyond $[\underline{z}_m, \overline{z}_m]$, then $\mathbf{z}_{im}$ is the final global optimal integer solution. Otherwise, use $[\underline{z}_m, \overline{z}_m]$ as the updated lower and upper bounds for z_m. In a similar manner, let us assume that we are now searching at the layer of z_i from z_m. In other words, we have specific integer values for all the layers from z_m to z_{i+1}. Again, by following the same procedure as in (30), we must have

$$d_{ii}(z_i + s_i - z_i^f)^2 + T_c \leq C_{im}, \tag{32}$$

where

$$s_i = \sum_{j=i+1}^{m} l_{ji}(z_j - z_j^f),$$

$$T_c = \sum_{k=i+1}^{m} T_c^k,$$

$$T_c^k = d_{kk}\left\{ z_k + \sum_{j=k+1}^{m} l_{jk}(z_j - z_j^f) - z_k^f \right\}^2,$$

with $k = i+1, i+2, ..., m$. If $T_c > C_{im}$, one should return to the previous layer of z_{i+1} for a new integer value. Otherwise, we can then determine the new lower and upper bounds of z_i as follows:

$$\underline{z}_i = \lfloor -\sqrt{(C_{im} - T_c)/d_{ii}} - s_i + z_i^f \rfloor, \tag{33a}$$

$$\overline{z}_i = \lceil \sqrt{(C_{im} - T_c)/d_{ii}} - s_i + z_i^f \rceil, \tag{33b}$$

which are used to update the previous lower and upper bounds of z_i and to continue the search for the global optimal integer solution to (5). Actually, the condition of $T_c > C_{im}$ is widely used in GPS ambiguity resolution to avoid extra computation so far as a combination of GPS ambiguity unknowns is found not to be a solution [18].

When $i = 1$, we start checking the candidates of z_1, given the values of $z_i\,(i = 2, 3, ..., m)$. If a new improved suboptimal integer solution is found, we update C_{im} and $\mathbf{z}_{im}$ and, accordingly, further update all the searching windows of $z_i\,(i = 1, 2, ..., m)$ with the newly improved value C_{im}; otherwise, after finishing searching the first layer of z_1, go to the next value of z_2. In case that all the candidates of z_2 have been tested, go to the next value of z_3. This searching procedure is repeated until the final global optimal integer solution is found. We should note that the searching windows for $z_i\,(i = 1, 2, ..., m)$ have been dynamically shrunken. In other words, if we denote the shrunken window by $[\underline{z}_i^s, \overline{z}_i^s]$ for the ith component of $\mathbf{z}$, then we must have $r_i = (\overline{z}_i^s - \underline{z}_i^s)/(\overline{z}_i^0 - \underline{z}_i^0) \leq 1$. Since LAMBDA depends on the initial searching window $[\underline{z}_i^0, \overline{z}_i^0]$, the searching strategy by Fincke and Pohst [8] is much faster than LAMBDA in the sense that the ratio of integer candidates to be checked by both methods is roughly equal to $\prod_{i=1}^{m} r_i \leq r_{\max}^m$, where $r_{\max}$ is the maximum value of all r_i.

The searching strategy of Fincke and Pohst [8] is to scan each layer of z_i from left to right, namely, starting from $\underline{z}_i$ and incrementally moving to the end of $\overline{z}_i$. Alternatively, Schnorr and Euchner [29] suggested that the searching at each layer starts from the middle of the interval $[\underline{z}_i, \overline{z}_i]$ and progressively moves oscillatorily to the two ends of $\underline{z}_i$ and $\overline{z}_i$. For example, if $[\underline{z}_i, \overline{z}_i] = [-4, 4]$, then the searching ordering should be arranged in the order of 0, $(1, -1)$, $(2, -2)$, $(3, -3)$ and finally $(4, -4)$. This oscillatory searching order at each layer by Schnorr and Euchner [29] has been shown to significantly improve the searching efficiency of the algorithm by Fincke and Pohst [8] and has since been widely implemented and used to find the global optimal integer solution to the ILS problem (5). For more details, one can refer to Fincke and Pohst [8] and Schnorr and Euchner [29].

Now the question is whether the efficiency of the wonderful combined algorithm by Fincke and Pohst [8] and Schnorr and Euchner [29], as discussed above, can be further improved. As is well known, sorting can significantly and/or even fundamentally affect the efficiency of an algorithm in scientific computation. Indeed, the contributions of Schnorr and Euchner [29] to the algorithm by Fincke and Pohst [8] are twofold: (i) to abandon the strategy of scanning integer candidates from one end to the other end but to re-order them in a zigzagged way from the center of the searching window; and (ii) to re-arrange the integer unknowns according to the reduced weight matrix. These two modifications have resulted in a profound improvement of speed to find the exact integer solution. Obviously, the techniques by Schnorr and Euchner [29] can be interpreted in terms of sorting applied both to $\mathbf{z}$ itself and the searching window for each z_i.

The great success of Schnorr and Euchner [29] motivates us to explore different sorting or re-ordering strategies for the integer unknowns themselves and to further develop the combined algorithm. Actually, almost all widely used solution algorithms implement some kind of strategy to re-order the integer unknowns. For example, the combined algorithm sorts the integer unknowns in the increasing order of the diagonal elements of $\mathbf{W}_f$, which will be referred to as the ascending sorting strategy. The LAMBDA algorithm arranges the unknowns according to the accuracy of the reduced floating-point solution. By assuming a unit weight matrix $\mathbf{W} = \mathbf{I}$ of $\mathbf{y}$, Damen et al. [7] applied reduction to the coefficient matrix $\mathbf{B}$ and then used the V-BLAST ordering to re-arrange the integer unknowns. In this section, we will extend the V-BLAST sorting strategy to a general weight matrix $\mathbf{W}$ of $\mathbf{y}$. Since the sorted QR ordering [42],[51-52] can significantly affect the performance of a suboptimal integer solution, we will also implement it and see how it can affect the performance of finding the exact integer solution.

To summarize, we assemble all the advantages of strategies either used for constructing a suboptimal integer solution or for searching the exact global optimal integer solution together to improve the combined algorithm by Fincke and Pohst [8] and Schnorr and Euchner [29] and the pseudo-codes are listed in Algorithm 4. More precisely, Algorithm 4 attempts to solve the ILS problem (5) by fully implementing all the advantages of lattice reduction/decorrelation, the early termination strategy and the dynamical shrinking of a searching window size by Fincke and Pohst [8] and the oscillatory ordering of searching window for each integer from the middle to the ends by Schnorr and Euchner [29], together with the sorted QR and/or V-BLAST orderings by Xu et al. [51-52], Wübben et al. [42] and Golden et al. [11]. We should note, however, that in the case of a high dimensional $\mathbf{z}$, if one would only be interested in the suboptimal integer solution of the sorted QR or V-BLAST type, one can immediately stop at Step S4 and continue to construct the suboptimal integer solution, as formulated in (12).

Algorithm 4: Algorithm to solve the ILS problem (5)

S1 **Input:** $\mathbf{W}_f$, $\mathbf{z}_f$ and C
S2 Reduce and represent $\mathbf{W}_f$ as $\mathbf{G}\mathbf{W}_r\mathbf{G}^T$. $\mathbf{z}_g = \mathbf{G}^T\mathbf{z}$ and $\mathbf{z}_r = \mathbf{G}^T\mathbf{z}_f$
S3 Apply sorted QR or V-BLAST ordering to $\mathbf{W}_r$, re-arrange $\mathbf{z}_g$ and $\mathbf{z}_r$
S4 Cholesky-decompose $\mathbf{W}_r$ into $\mathbf{L}\mathbf{D}\mathbf{L}^T$
S5 **Initialize:** $i \leftarrow m$, $C_{im} \leftarrow C$;
and without confusion, $\mathbf{z} \leftarrow \mathbf{z}_g$ and $\mathbf{z}_f \leftarrow \mathbf{z}_r$
compute $[\underline{z}_m, \overline{z}_m]$ by (31), arrange the integers of z_m
from middle to ends into a vector $\mathbf{z}_m^*$, and $z_i \leftarrow \mathbf{z}_m^*(1)$
S6 Compute T_c
S7 **if** $T_c > C_{im}$, increase i for the next integer of z_i.
S8 **if** $z_i \in [\underline{z}_i, \overline{z}_i]$, go to Step S6;
S9 **else**
if $i = m$, output the solution $\mathbf{z}_{im}$ and go to Step S17, **end**;
increase i for the next integer of z_i
go to Step S8.
S10 **end**
S11 **else** $i \leftarrow (i-1)$. Compute $[\underline{z}_i, \overline{z}_i]$ and $z_i \leftarrow \mathbf{z}_i^*(1)$;
S12 **if** $i = 1$
S13 for each $z_1 \in [\underline{z}_1, \overline{z}_1]$, compute $T_c^1 + T_c$ and
update C_{im} via $C_{im} \leftarrow T_c^1 + T_c$ if $T_c^1 + T_c \leq C_{im}$
store/update the intermediate integer solution $\mathbf{z}_{im}$
after searching this layer, take the next value of z_2 and $i \leftarrow 2$.
S14 **end**
S15 go to Step S8;
S16 **end**
S17 **Output:** Use the solution $\mathbf{z}_{im}$, the ordering information of Step S3 and $\mathbf{G}$ to recover the final ILS solution.

To demonstrate efficiency improvement by sorted QR and V-BLAST and to give the reader a comparative idea on the performances of the LAMBDA method by Teunissen [36] and the combined algorithm by Fincke and Pohst [8] and Schnorr and Euchner [29], we show the following real-life GPS example of a baseline of about 70 meters, whose $\mathbf{W}_f$ matrix and the associated floating solution $\mathbf{z}_f$ are respectively listed as follows:

$$\mathbf{W}_f = \begin{bmatrix} 35.7965 & 18.9907 & -4.5070 & -33.0745 & -2.9469 & -6.1174 & 0.0072 & -15.8043 \\ 18.9907 & 28.5008 & -5.8801 & -8.0326 & 8.3884 & -24.1421 & -20.0832 & -0.5780 \\ -4.5070 & -5.8801 & 62.5920 & 1.5891 & -8.8773 & 8.9281 & -22.7657 & -27.6485 \\ -33.0745 & -8.0326 & 1.5891 & 50.1116 & 4.8221 & -24.9918 & 7.1409 & 2.3000 \\ -2.9469 & 8.3884 & -8.8773 & 4.8221 & 75.9902 & 9.4921 & -8.6107 & -10.1608 \\ -6.1174 & -24.1421 & 8.9281 & -24.9918 & 9.4921 & 58.9446 & 0.9111 & 7.0683 \\ 0.0072 & -20.0832 & -22.7657 & 7.1409 & -8.6107 & 0.9111 & 60.6125 & -23.2253 \\ -15.8043 & -0.5780 & -27.6485 & 2.3000 & -10.1608 & 7.0683 & -23.2253 & 56.1006 \end{bmatrix},$$

$$\begin{aligned} \mathbf{z}_f \quad = \quad & (-1299632.965 \;\; 1351127.969 \;\; 847614.001 \;\; -1544660.986 \\ & -290017.996 \;\; -2417696.014 \;\; 2252905.995 \;\; -4816275.991)^T. \end{aligned}$$

Based on this example, we set two different values for C to show its effect on the speed to find the exact solution. Keeping in mind that not all problems can be successfully decorrelated by any existing reduction/decorrelation methods ([45],[50]), we also design two scenarios with and without reduction/decorrection. To be scientifically fair for all the methods under comparison, we implement a variant of LLL algorithm to decorrelate $\mathbf{W}_f$. We then conduct the experiments with LAMBDA (version 2.0b of 1999), the combined algorithms with and without the ascending ordering strategy, and the improved methods with the incorporation of the sorted QR and V-BLAST orderings. Listed in Table 1 are the total numbers of integer candidates that must be checked by each of the algorithms

under comparison to find the global optimal integer solution (compare column "Opt" of Table 1). Since geodesists are concerned with the second optimal integer solution, we also show the total numbers of integer candidates that have to be tested by each algorithm to find the second optimal solution (compare column "2Opt" of Table 1).

Table 1: Total numbers of integer candidates that have been checked with two different values of C by each of the following algorithms: the combined algorithms [8],[29] with and without the ascending ordering, the LAMBDA method [36], the improved algorithms with the implementation of either the sorted QR or V-BLAST ordering, which are denoted by SUPER1, SUPER2, LAMBDA, Improved1 and Improved2, respectively.

Methods	Reduction	SUPER1		SUPER2		LAMBDA		Improved1		Improved2	
		Opt	2Opt	Opt	2Opt	Opt	2Opt	Opt	2Opt	Opt	2Opt
C_1 :	Yes	8	17	8	17	14	24	8	17	8	17
10.2451	No	8	118	8	223	161	320	8	106	8	88
C_2 :	Yes	8	17	8	17	24711	49301	8	17	8	17
100.2451	No	8	147	8	277	49224	98525	8	136	8	108

It is clear from Table 1 that given the two values of C, the combined algorithm by Fincke and Pohst [8] and Schnorr and Euchner [29] and the improved methods with either of the sorting strategies (sorted QR and V-BLAST) have an excellent performance in finding the global optimal integer solution. They are significantly faster than LAMBDA by a factor from 75 per cent to 3088 in the case of a decorrelated $\mathbf{W}_f$ and by a factor from 20 to 6152 in the case of a non-decorrelated $\mathbf{W}_f$. This latter case is not superficial, since simulations have clearly indicated that not all $\mathbf{W}_f$ with a reasonably large condition number can be successfully decorrelated by any reduction/decorrelation methods available in the literature up to the present ([45],[50]). If the second optimal integer solution is to be sought, the improved methods perform clearly better than the combined algorithms by Fincke and Pohst [8] and Schnorr and Euchner [29] in the case of the original $\mathbf{W}_f$. It is also obvious from Table 1 that the combined algorithm with the ascending sorting strategy performs significantly better than that without the same sorting strategy. We also test the combined algorithm by sorting $\mathbf{z}$ in the decreasing order of the weights of the floating solution. The searching speeds are a few times slower than those reported in Table 1, when the second optimal solution is sought. Thus the results are not reported here. The sorting strategy V-BLAST in column Improved2 performs better than the sorted QR ordering in column Improved1; nevertheless, V-BLAST requires much more time than the sorted QR to obtain the ordering of $\mathbf{z}$.

Finally, to summarize the similarity and/or difference among the exact searching methods, we show the features of each algorithm/method in Table 2. The abbreviations used in Table 2 are explained as follows. SUPER1, SUPER2, LAMBDA, Improved1 and Improved2 have been defined as in Table 1. FPohst stands for the method proposed by Fincke and Pohst (1985); ScanE2E for scanning the candidates of each integer from end to end; DynShrink for dynamical shrinking; ScanZZ for scanning the candidates of each integer in a zigzagged manner; SortingZ for sorting all the integer unknowns in the sense of minimum conditional variance and/or maximum conditional weight. In addition, DESC stands for sorting $\mathbf{z}$ in the decreasing order of the diagonal elements of $\mathbf{W}_f$; ASCEW for the ascending sorting strategy; DESCV for sorting $\mathbf{z}$ according to the variances of the floating solution; SortedQR for the sorted QR strategy and VBLAST for the V-BLAST ordering.

Table 2: Features and/or components used by each of the exact ILS methods.

Methods	FPohst	SUPER1	SUPER2	LAMBDA	Improved1	Improved2
ScanE2E	✓			✓		
DynShrink	✓	✓	✓		✓	✓
Reduction	✓	✓	✓	✓	✓	✓
ScanZZ		✓	✓		✓	✓
SortingZ	DESC	ASCEW		DESCV	SortedQR	VBLAST

6 Concluding remarks

The mixed integer linear model (1) or the integer linear model (2) is a starting basis of integer statistical inference. Although the real-valued linear model has been well documented both in standard books on statistics and in publications in professional journals of statistics, statisticians have contributed very little to the study of (1) or (2). Estimating integer unknowns from noisy data has been becoming increasingly important for highly interdisciplinary applications. Very often, scientists and engineers from different discipline publish their research results in journals within their own community and in different languages or terminologies. As a result, researchers from one area of science/engineering may not realize any progress achieved by other researchers from other areas of science/engineering, even though they are all dealing with (1) and/or (2).

We have discussed the methods for estimating integer unknowns from noisy data from an applications-oriented point of view. When the least squares method or the maximum likelihood is applied to (1) or (2), we can derive the ILS problem or equivalently, the weighted closest point problem. Since the ILS problem is NP-hard, there exist no algorithms to find the exact solution in polynomial time. Thus for high dimensional problems, one may only expect a suboptimal integer solution. We have shown a unified scheme to derive such a suboptimal integer solution, whose quality depends on how the positive definite matrix $\mathbf{W}_f$ is re-organized and decomposed. Two most successful ordering schemes are the sorted QR ordering proposed by Xu et al. [51] and independently by Wübben et al. [42] and the V-BLAST ordering proposed by Bell Laboratories (see, e.g., [11]). For low dimensional problems, the most popular and powerful searching method originated from Fincke and Pohst [8] and was further developed by Schnorr and Euchner [29], which essentially consists of four basic elements, namely, (i) reduction/decorrelation, (ii) dynamically improving the size of searching window, (iii) scanning (or equivalently, sorting the ordering of) the integer candidates of each integer unknown in the zigzagged manner; and (iv) sorting the integer unknowns in the ascending order of the diagonal elements of the weight matrix.

The sorted QR [42],[51-52] and V-BLAST [11] ordering strategies have been successfully used to construct suboptimal integer solutions. From the statistical point of view, these two ordering strategies are to re-order or sort the integer unknowns on the basis of maximum conditional weighting and minimum conditional variance, respectively. In this paper, we have assumed a general weight matrix $\mathbf{W}$ of $\mathbf{y}$, incorporated these two sorting strategies into the combined algorithm and further improved it to find the global optimal integer solution. All the basic ideas in this paper can naturally be used either to construct reduction-aided suboptimal integer solutions for high dimensional problems or to find the exact solution for low dimensional problems. In this latter case, the test examples have clearly shown that: (i) the popular combined algorithm performs significantly better than LAMBDA by a factor from 75 per cent to 6152, depending on the chosen C value and the condition of $\mathbf{W}_f$; and (ii) the improved methods are clearly better than the popular combined algorithm when searching for the optimal and second optimal integer solutions, if $\mathbf{W}_f$ cannot be well reduced. We should note,

however, that although the V-BLAST ordering is shown to perform better than the sorted QR, such an advantage should not be over-emphasized, since this ordering requires much more time to compute.

Acknowledgement: We are very grateful to Mr. Z.G. Hu, Wuhan University, for providing all the computation of the GPS example. We also thank the two reviewers very much for their constructive comments. This work is partially supported by the 111 Project B07037, PRC Ministry of Education and Project 863-2007AA120603 of the National High Technology Research and Development Program of China.

References

1. Blewitt G., 1989. Carrier phase ambiguity resolution for the Global Positioning System applied to geodetic baselines up to 2000 km. *J. geophys. Res.*, B94:10187-10203.

2. Brunetti S. and Daurat A., 2003. An algorithm reconstructing convex lattice sets. *Theor. Comput. Sci.*, 304:35-57.

3. Cassels J.W.S., 1971. *An Introduction to the Geometry of Numbers*, Springer, Berlin.

4. Chang X.W., Yang X. and Zhou T., 2005. MLAMBDA: a modified LAMBDA method for integer least-squares estimation. *J. Geod.*, 79:552-565.

5. Chen D.S., 1994. Development of a fast ambiguity search filtering (FASF) method for GPS carrier phase ambiguity resolution. PhD dissertation, UCGE Reports 20071, The University of Calgary.

6. Dahiya R.C., 1981. An improved method of estimating an integer-parameter by maximum likelihood. *Amer. Stat.*, 35:34-37.

7. Damen M.O., Gamal H.E. and Caire G., 2003. On maximum-likelihood detection and the search for the closest lattice point. *IEEE Trans. Inf. Theory*, 49:2389-2402.

8. Fincke U. and Pohst M., 1985. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Math. Comput.*, 44:463-471.

9. Gardner R.J., Gritzmann P. and Prangenberg D., 1999. On the computational complexity of reconstructing lattice sets from their X-rays. *Discrete Math.*, 202:45-71.

10. Ge M.R., Gendt G., Rothacher M., Shi C. and Liu J., 2008. Resolution of GPS carrier-phase ambiguities in precise point positioning (PPP) with daily observations. *J. Geod.*, 82:389-399.

11. Golden G.D., Foschini C.J., Valenzuela R.A. and Wolniansky P.W., 1999. Detection algorithm and initial laboratory results using V-BLAST space-time communication architecture. *Electron. Lett.*, 35:14-16.

12. Grafarend E.W., 2000. Mixed integer-real valued adjustment (IRA) problems: GPS initial cycle ambiguity resolution by means of the LLL algorithm. *GPS Solut.*, 4:31-44.

13. Gruber P.M. and Lekkerkerker C.G., 1987. *Geometry of Numbers*, North-Holland, Amsterdam.

14. Hassibi A. and Boyd S., Integer parameter estimation in linear models with applications to GPS. *IEEE Trans Signal Proc.*, 46:2938-2952.

15. Helfrich B., 1985. Algorithms to construct Minkowski reduced and Hermite reduced lattice bases. *Theor. Comput. Sci.*, 41:125-139.

16. Hofmann-Wellenhof B., Lichtenegger H. and Collins J., 1992. *GPS — Theory and Practice*. Springer-Verlag, Berlin.

17. Joux A. and Stern J., 1998. Lattice Reduction: A Toolbox for the Cryptanalyst. *J. Cryptology*, 11:161-185.

18. Landau H. and Euler H.-J., 1992. On-the-fly ambiguity resolution for precise differential positioning. in: *Proc. ION GPS92*, Albuquerque, pp.607-613.

19. Lenstra A.K., Lenstra H.W. and Lovász L., 1982. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515-534.

20. Lu G., 1995. Development of a GPS multi-antenna system for attitude determination. PhD dissertation, UCGE Reports 20073, The University of Calgary.

21. Miller G.K., 1999. Maximum likelihood estimation for the Erlang integer parameter. *Stat. Prob. Lett.*, 43:335-341.

22. Nemhauser G. and Wolsey L., 1988. *Integer and Combinatorial Optimization*, Wiley, New York.

23. Nguyen P.Q. and Stehle D., 2004. Low-dimensional lattice basis reduction revisited, in ANTS 2004, LNCS 3076, pp.338-357, Springer, Berlin.

24. Nguyen P.Q. and Stehlé D., 2006. LLL on the average, in: *ANTS 2006, LNCS 4076*, eds. F. Hess, S. Pauli and M. Pohst, Springer, Berlin, pp.238-256.

25. Nguyen P.Q. and Stehlé D., 2009. An LLL algorithm with quadratic complexity. *SIAM J. Comput.*, 39:874-903.

26. Nguyen P.Q. and Vallée B.(eds), 2010. *The LLL Algorithm — Survey and Applications*, Springer, Berlin.

27. Regev O., 2009. On Lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56:34:1-34:40.

28. Scharlau W. and Opolka H., 1985. *From Fermat to Minkowski*, Springer, New York.

29. Schnorr C.P. and Euchner M., 1994. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Math. Prog.*, 66:181-199.

30. Shannon C.E., 1959. Probability of error for optimal codes in a Gaussian channel. *Bell System Techn. J.,* 38:611-656.

31. Smeets I., 2010. The history of the LLL-algorithm, in: *The LLL Algorithm*, eds. P.Q. Nguyen and B. Vallée, Springer, Berlin, pp.1-17.

32. Stark A.E., 1975. Some estimators of the integer-valued parameter of a Poisson variate. *J. Amer. Stat. Assoc.*, 70:685-689.

33. Taha H., 1975. *Integer Programming – Theory, Applications, and Computations*, Academic Press, New York.

34. Teunissen P.J.G., 1993. Least-squares estimation of the integer GPS ambiguities, in: LGR-Series No.6, Delft Geodetic Computing Centre, pp.59-74, Delft University of Technology.

35. Teunissen P.J.G., 1994. A new method for fast carrier phase ambiguity estimation. in: *Proc. IEEE PLANS'94*, Las Vegas, Nevada, April 11-15, pp.562-573.

36. Teunissen P.J.G., 1995. The least-squares ambiguity decorrelation adjustment: A method for fast GPS integer ambiguity estimation. *J. Geod.*, 70:65-82.

37. Teunissen P.J.G., 1999. An optimality property of the integer least-squares estimator. *J. Geod.*, 73:587-593.

38. Waters D.W. and Barry J.R., 2005. A reduced-complexity lattice-aided decision-feedback detector, *Proc. 2005 Int. Conf. Wireless Networks, Communications and Mobile Computing,* pp.845-850.

39. Waters D.W. and Barry J.R., 2005. Noise-predictive decision-feedback detection for multiple-input multiple-output channels. *IEEE Trans. Signal Proc.*, 53:1852-1859.

40. Vallée B., 1991. Gauss' algorithm revisited. *J. Algorithm,* 12:556-572.

41. Sikiric M.D., Schurmann A. and Vallentin F., 2009. Complexity and algorithms for computing Voronoi cells of lattices. *Math. Comput.*, 78:1713-1731.

42. Wübben D., Böhnke R., Rinas J., Kühn V. and Kammeyer K.D., 2001. Efficient algorithm for decoding layered space-time codes. *Electronics Lett.*, 37:1348-1350.

43. Wübben D., Böhnke R., Kühn V., and Kammeyer K.D., 2003. MMSE extension of V-BLAST based on sorted QR decomposition, *Proc. IEEE 58th Vehicular Technology Conference, VTC 2003-Fall,* vol.5, pp.508-512.

44. Xu P.L., 1998. Mixed integer geodetic observation models and integer programming with applications to GPS ambiguity resolution. *J. Geod. Soc. Japan*, 44:169-187.

45. Xu P.L., 2001. Random simulation and GPS decorrelation. *J. Geod.*, 75:408-423.

46. Xu P.L., 2002. New Challenges in Connection with Precise GPS Positioning, in: *Proc IAG*, vol.125, (invited but fully reviewed), pp.359-364.

47. Xu P.L., 2003. Voronoi cells, probabilistic bounds and hypothesis testing in mixed integer linear models, paper presented at IUGG 2003, June 30 - 11 July, Sapporo, Japan.

48. Xu P.L., 2006. Voronoi cells, probabilistic bounds and hypothesis testing in mixed integer linear models. *IEEE Trans Information Theory*, 52:3122-3138.

49. Xu P.L., 2010. Mixed integer linear models, Ch.38, in: *Handbook of Geomathematics*, eds. W. Freeden, Z. Nashed and T. Sonar, pp.1129-1157, Springer, Berlin.

50. Xu P.L., 2012. Parallel Cholesky-based reduction for the weighted integer least squares problem, *J. Geod.*, 86:35-52, DOI 10.1007/s00190-011-0490-y.

51. Xu P.L., Cannon E. and Lachapelle G., 1995. Mixed integer programming for the resolution of GPS carrier phase ambiguities, presented at IUGG95 Assembly, Boulder, July 2-14, 1995. Also available as arXiv:1010.1052v1[cs.IT]

52. Xu P.L., Cannon E. and Lachapelle G., 2000. Mixed integer observation models, GPS decorrelation and integer programming, Technical Report Nr.2000.2, Geodetic Institute, Stuttgart University.